Modeling and Simulation of Worm Propagation and Attacks against Campus Network

Rashid Husain, Bishir Suleiman

***Abstract*— We develop a model of worm attack against campus network in accordance with the campus signal flow as committed by an external attacker (or intruder) and examine the worm-flow behavior and its rate of infection. Modeling and simulation are two basic integral components employed to test-run the model using Optimized Network Engineering Tool (OPNET) and two forms of statistical events were considered. The object statistics is mainly comprised of our modeled Campus network signal flow plus the attacker and the Global statistics gives an account of the result of the simulation as it shows the number of infected host systems over the network under consideration. We further analyze the result from three perspectives, namely: ''As Is, Multiplier and Average.'' We recommend that the infection rate of worm viruses be investigated from an attacker situated or positioned internal to the network (i.e. an authorized user distributing worm) under consideration.**

***Index Terms*— Model, Worm, Signal-Flow, Intruder, OPNET, Object statistics, Global Statistic**

I. Introduction

1.1 Model

A model is a logical representation of a system [1, 5]. A system is understood to be an entity which maintains its existence through the interaction of its parts. A model is a simplified representation of the actual system intended to promote understanding. Figure 1 demonstrates the Model Taxonomy [14], in this figure Models are divided into four major parts: Deterministic models, stochastic models, Rule based models and Multi-agent models.

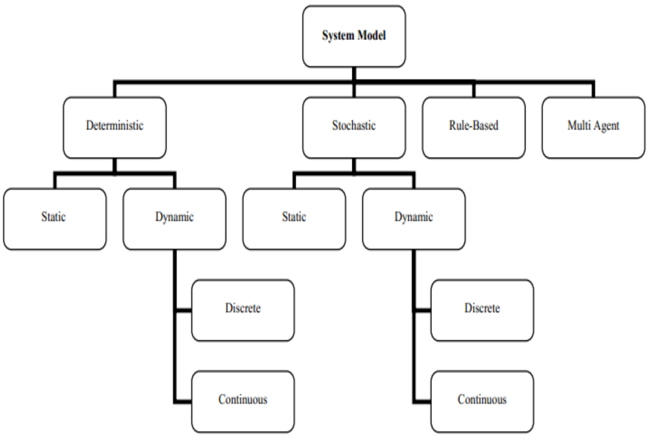

Fig. 1: Model Taxonomy

1.2 Simulation

Simulation is the manipulation of a model in such a way that it represents the behavior of system. Simulation is a cost-effective tool for exploring new systems without having to build them. Simulation can be categorized into three parts [10, 14]:

i. Live Simulation: Simulating real entities (people and/or equipments) in the real world, in the field of IS Packet wars and Role Paying are examples of Live Simulation.

ii. Virtual Simulation: Simulating real entities in a virtual world.

iii. Constructive Simulation: Simulating virtual entities, usually in a virtual world. In the field of IS Sniffers and canned attack/defend scenarios are Constructive Simulation.

1.3 Modeling and Simulation: Is a discipline for developing a level of understanding of the interaction of the parts of a system, and the system as a whole. The results of Modeling and Simulation can help Information Security in many areas including [16]: Analyzing the Risks of Information Security Investments, Predicating the future in the field of IS (Vulnerability Risk Assessment), Simulating the process of Malicious Codes propagating, Evaluating the security topologies in computer systems, etc. we can summarize these applications as :

i. Testing both attack and defense
ii. Analysis of intrusions and attacks
iii. Research and Development (R&D) of new countermeasures In the field of IS we encounter with complex systems to simulate, in these cases we need techniques to break the system into subsystems, DOD (Department of Defense) developed a technical framework to make it easier for all kinds of simulation models In order to solve the problems of traditional simulation models (The lack of reusability and interoperability), DOD developed High Level Architecture (HLA) [2, 10]. HLA connects several computer-based simulation systems so that they can run together and exchange information. Instead of building a big monolithic simulation system from scratch, the HLA allows engineers to combine existing simulation systems with new systems. HLA enables them to reuse existing systems for new purposes. They can also mix different programming languages and operating systems.

II. Current State of Modeling and Simulation in the Field of Information Security

As mentioned earlier, there is not any explicit Modeling and Simulation tool for testing computer security and network attack modeling. There are some special purpose tools for modeling and Simulating of Information Security. For

Rashid Husain, Lecturer, Department of Mathematics and Computer Science, Faculty of Natural and Applied Sciences, Umaru Musa Yar'adua University Katsina State-Nigeria.
Bishir Suleiman, Research Scholar, Department of Mathematics and Computer Science, Faculty of Natural and Applied Sciences, Umaru Musa Yar'adua University Katsina State-Nigeria.

Modeling and Simulation in the field of IS, we can use Network Simulators. These tools are: OPNET, NS-2, Cnet, Netrule, etc. But Network Simulators are poor choices when it comes to simulating computer security and network attacks. There are significant limitations to applying modeling and simulation when it comes to security issues. Simulation of information security divides into five distinct categories [3, 13]:

i. Packet wars (Example: IWAR)

Information Warfare Analysis and Research (IWAR) categorized into three [4, 9]:

- Computer Network Attack
- Computer Network Defense
- Computer Network Exploitation

ii. Network Design Tools: (Example: OPNET)

iii. Canned Attack/Defend Scenarios: (Example: MAADNET)

iv. Management Flight Simulators: (Example: EASEL)

v. Role-Playing

2.1 Network Design Tools: (Example: OPNET)

Optimized Network Engineering Tool (OPNET) is a sophisticated M&S tool with the specific purpose to construct, simulate, and evaluate communication network design (topologies with specific devices), configurations of network nodes the transmission of packets through the network, and the use of different network protocols all from a performance point of view.

OPNET was developed by MIT [5, 12]. OPNET consists of four different editors:

1- Network Editor: To Design Network Topology

2- Node Editor: Data Flow are defined here

3- Process Editor: is used for describing logic flows and behaviors

4- Parameter Editor (utility editor):

The essential part of OPNET that is used for simulating Security is Net Doctor. Net Doctor is used mainly for analyzing network security with focus on policies and configuration testing. Utilizing Net Doctor help engineers to audit and validate network devices configuration for misconfiguration, and it helps an administrator for troubleshooting of network devices. Mis-configured network devices are a big security risk within the network environment and figures saying 40% of security related issues are caused by misconfigured network devises and servers. In the following, there are some advantages of Net Doctor: [3, 7]

1- Analyze Network Health

2- Detect Configuration problems

3- Enforce Organizational Policies in the network

4- Automate the process of Audit and Validation

2.2 Major drawbacks with OPNET are: [4, 6]

1- Lack of truthful (Verified and Validated) Attacks Models DoS and DoS attacks can be tested because a TCP/IP stack is implemented in OPNET but if buffer overflows, race conditions, viruses, and worms are going to be tested we need models

2- Problems with modeling network traffic

2.3 Vulnerabilities, Threats, and Attacks [10, 14]

When discussing network security, the three common terms used are as follows:

2.3.1 Vulnerability: A weakness that is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves [6]. The vulnerabilities are present in the network and individual devices that make up the network. Networks are typically plagued by one or all of three primary vulnerabilities or weaknesses:

- Technology weaknesses
- Configuration weaknesses
- Security policy weaknesses

2.3.2 Threats: The people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses. There are four primary classes of threats:

- Structured threat
- Unstructured threat
- Internal Threat
- External Threat

2.3.3 Attacks: The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Four primary classes of attacks exist [11]:

- Reconnaissance
- Access
  - Password attacks
  - Trust exploitation
  - Port redirection
  - Man-in-the-middle attacks
  - Social engineering
  - Phishing
- Denial of service
- Worms, viruses, and Trojan horses

2.3.4 Attack Tools

Password cracking software
Port Scanner
Network Sniffers
Buffer Flow Vulnerability
Viruses and Worms
Protocol Exploit
Trojan Horses

2.3.5 Defense Tools

Intrusion Detection System and Firewall
Cryptograph, Encryption and Decryption Techniques
System Application and Protocol wrappers
Honey pots
Forensic analysis tools

2.3.6 Access Control Method

The firewalls: Are assuming to be immune to infection. It also assumed that we have sensors at the vulnerable hosts that can defeat an infection and report it [6, 7].

III. Case Study: Campus Network Attack Simulation

In this simulation, the campus network is “attacked” by an intruder externally situated to the network with a flooding attack. Two (2) routers are connected to a server which is further connected to seven (7) switches that form various LANs for existing Faculties and Departments. The campus network is successfully attacked due to network equipment weaknesses such as password protection, Lack of authentication, Routing protocols and in-built firewall holes. This Simulation contains the following components:

- Two (2) Mikrotik Routers
- Two (2) Servers
  - Web Server (HTTP, Telnet)

  - Cyber Effects Config
- One (1) System Admin.
- An Attacker
- One Application Profile
- Seven (7) Switches:
  - One at Campus Data Center
  - Two Senate Complex Building
  - One at Faculty of Humanities
  - One at Faculty of Education
  - Two at Faculty of Natural and Applied Sciences

Other sections are connected via Wireless Access Point such as Library, Staff quarters, Students Center, etc.

3.1 DDoS Attack: Modeling and Simulation by OPNET

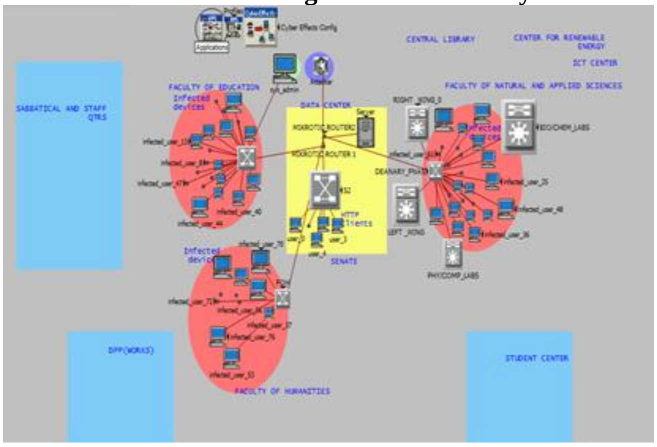

Fig. 2: Modeling and Simulation of Campus Network

IV. Result of Simulation

4.1 Object Statistics result

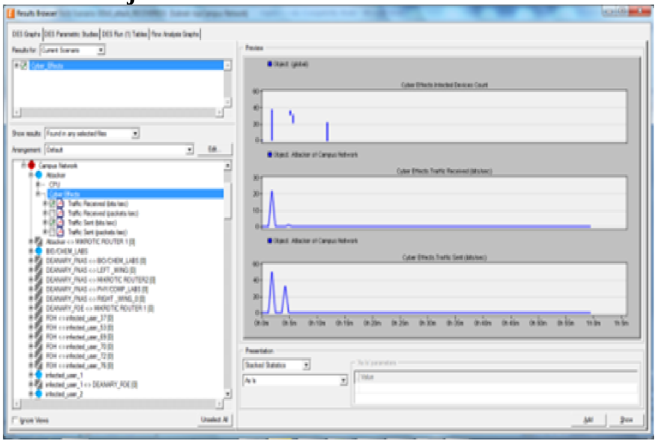

Fig. 3 Object statistics

4.2 Result of Simulation ('As Is' Global Statistics result)

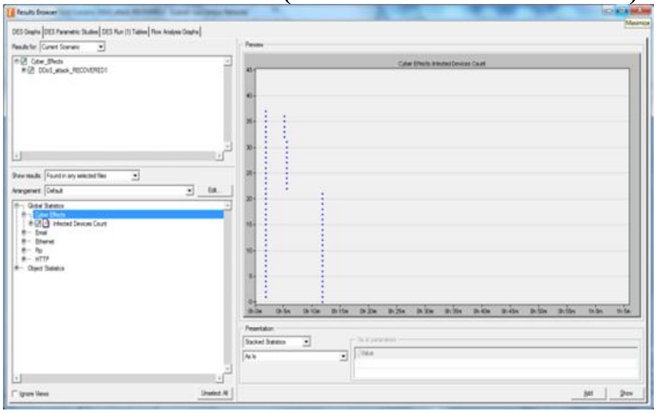

Fig. 4: 'As Is' Result

4.3 Multiplier' Result of Global Statistics

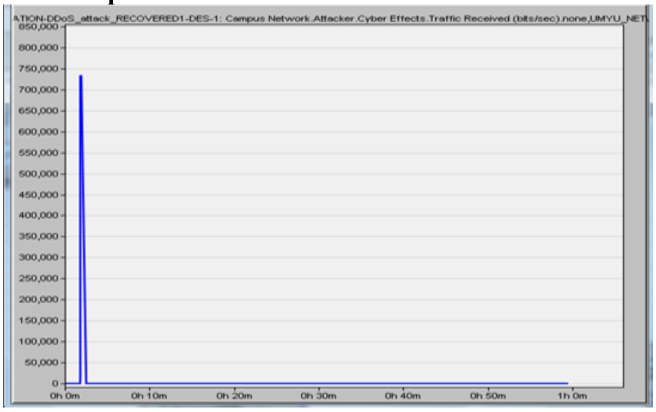

Fig. 5: 'Multiplier' Result

4.4 'Average' Result of Global Statistics

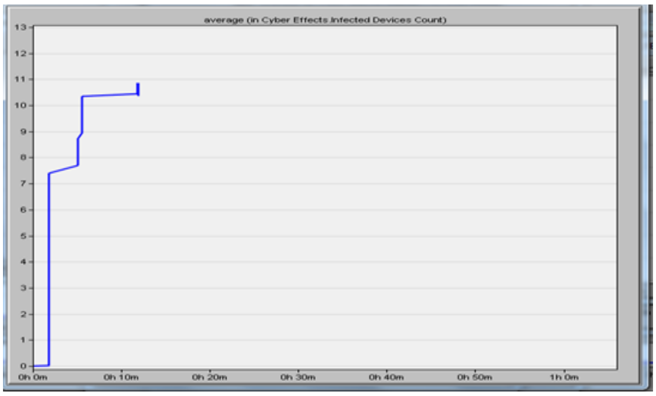

Fig. 6: 'Average' Result

V. Analysis of the Result

'As Is' result recorded zero infection for the first one hundred and eight seconds (108). The first device become infected after 109 seconds (simulation time) i.e. the total simulation time for this discrete analysis is about 24521 seconds with total infected device of 1369.

'Multiplier' result shows that about 109 seconds simulation time, 19861 devices were infected. Total execution time for multiplier about 202721 seconds with a total of infected devices about 13962517.

'Average' result analysis, we obtained that, at about 109 simulation time the first set of devices were infected. The total execution time was 24521 seconds with a total infected devices of about 480.

VI. Conclusion

The Campus network signal flow was model and simulated using optimize network engineering tool (OPNET). The attacker was situated at a position externally to the Campus network. The intruder attempts to penetrate the security of networks router despite its in-built firewall through firewall holes. The attacker makes such attempts severally until it becomes successful. Our results were categorized into three (3) namely; 'As Is', 'Multiplier', and 'Average'.

Recommendation

It is recommended that, the future work is first to investigate the rate of infection of computer worms from the point of view of an intruder that is positioned internal to the campus network.

REFERENCE

[1] David A. Cook. (2001). “Computers and M&S Modeling and Simulation”, *The Journal of Defense Software Engineering,* Vol. 4(5).

[2] Chris Turrell, (1999). “High Level Architecture Simulation Technology”, http://www.sisostds.org/webletter/siso/iss_18/.

[3] John H. Saunders. (2002). "Simulation Approaches in Information on Security Education", *in Proc. 6th National Colloquium for Information System Security Education, Redmond, WA.* http://cisse.info/CISSE%20J/2002/saun.pdf

[4] Daniel Ragsdale, John Hill, Scott Lathrop, and Gregory Conti. (2000). “*Information Assurance Program at West Point”*.

[5] Nicholas Weaver, (2002). “Future Defenses: Technologies to Stop the Unknown Attack Internet”, http://online.securityfocus.com/infocus/1547

[6] http://www.cisco.com/application/pdf/en/us/guest/products/ps5317/C2001/migration

[7] Suleiman B., Husain R. and Muhammad S., (2015). “A Study on Hierarchical Model of Computer Worm Defense System”, *International Journal of Engineering and Applied Sciences*, Vol. 2 (4), pp: 55-59.

[8] Nicholas Weaver, (2002). “Warhol Worms: The Potential for Very Fast Internet Plagues," UC Berkeley.

[09] Tarkan Yetiser, (1993). “Polymorphic Viruses Implementation, Detection and Protection," VDS Advanced Research Group.

[10] Dan Zerkle and Karl Levitt, (1996). “Netkuang - a multi-host con_guration vulnerability checker,” USENIX.

[11] Husain Rashid and Mansir Abubakar, (2015). “A Study on Friends Model of a Computer Worm Defense System”, IJEAS, Vol. 2(3), pp: 56-59.

[12] David Moore et al. (2003). “Inside the Slammer Worm," In IEEE Security and Privacy. [9] Carey Nachenberg, “Computer Parasitology," Symantec AntiVirus Research Center.

[13] Carey Nachenberg. “Understanding and Managing Polymorphic Viruses," Symantec AntiVirus Research Center.

[14] Don Seeley, (1989). “A Tour of the Worm," In Proceedings of 1989 Winter USENIX Conference, pp. 287 -304.

[15] John F. Shoch and Jon A. Hupp, (1982). ”The Worm Programs - Early Experience with a Distributed Computation," Communications of the ACM, Vol.25(3) pp: 172 -180.

[16] Eugene H. Spa_ord, (1988). “The Internet Worm Program: An Analysis," Technical Report CSD-TR-823, Purdue University, West Lafayette, IN, USA.